Security Evaluation of Physical RNGs

Werner Schindler

April 8, 2019

Keywords: random number generator (RNG), physical RNG, evaluation criteria, AIS 31.

Extended Abstract

Many cryptographic mechanisms and protocols require random numbers, e.g. to generate challenges, session keys, symmetric keys, signature parameters, random primes, ephemeral keys, nonces, blinding values and masking values, to name some important applications. Weak RNGs (random number generators) may allow an attacker to break cryptographic mechanisms even if they are principally strong. Sensitive cryptographic applications require strong (secure) RNGs. Thus appropriate evaluation criteria are needed.

A large number of RNG designs have been described and analysed in the literature. We distinguish between deterministic RNGs (a.k.a. pseudorandom number generators), physical RNGs (using dedicated hardware) and non-physical true RNGs (exploiting system resources or human interaction). These main classes can be divided into subclasses ('pure' and 'hybrid'). Representatives of the latter subclasses have properties of both, deterministic and true RNGs. Physical RNGs are typically implemented on smart cards and FPGAs. Well-known examples of non-physical true RNGs are /dev/random and /dev/urandom.

In the talk generic security requirements are motivated, and the main differences between the particular RNG classes are explained. The talk yet focuses on the evaluation of physical RNGs.

The concept of a stochastic model is developed and illustrated by examples. A stochastic model allows to estimate the (average) entropy of the random numbers, or more precisely, the average entropy of the describing random variables. Due to tolerances of the components or ageing effects the quality of the random numbers, which are generated by a particular device in operation, may be lower than the quality of the random numbers, which were generated by carefully investigated prototypes. Also, a total failure of the noise source might occur (e.g. because a defective flip flop outputs constant values). Such events, an in-

acceptable quality of the random numbers or a total failure of the noise source, must be detected reliably and sufficiently soon by appropriate online tests and tot tests. Differences to the evaluation of non-physical true RNGs are briefly mentioned.

The Common Criteria do not provide a concrete evaluation methodology for RNGs. In the German certification scheme evaluation guidelines for deterministic RNGs (AIS 20) and for physical RNGs (AIS 31) have been effective since 1999, resp. since 2001. In 2011 the corresponding mathematical-technical documents were updated. The AIS 31 is also applied in the French certification scheme, and certificates, which confirm the PTG.2 conformance of an RNG, have mutually been recognized for more than three years.

The requirements and the security goals of the most relevant functionality classes of the AIS 20 and AIS 31 are explained and typical applications are given, for which the generated random numbers are appropriate. Experiences from almost two decades and the impact of the AIS 31 are pointed out. Finally, some national and international standards and evaluation documents are discussed briefly, and similarities and differences to the AIS 31 are mentioned.

References

[1] AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren. Anwendungshinweise und Interpretationen zum Schema (AIS), Version 3 (15.05.2013) (mandatory if a German IT security certificate is applied for).
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf

[2] AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. Anwendungshinweise und Interpretationen zum Schema (AIS), Version 3 (15.05.2013) (mandatory if a German IT security certificate is applied for).
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf

[3] W. Killmann, W. Schindler: A Proposal for: Functionality Classes for Random Number Generators. Version 2.0 (18.09.2011), mathematical-technical reference of the AIS 20 and AIS 31.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_evaluation_methodology_for_true_RNG_e.pdf